

2007-CDOS-DIE-001-0402

**PREMIER ELECTION
SOLUTIONS
(FORMERLY DIEBOLD)**

**PROJECT
OVERVIEW**

“A.3”

COPY

2007-CDOS-DIE-001-0402
PROJECT OVERVIEW BINDER “A.3”

TABLE OF CONTENTS

2007-CDOS-DIE-001-0402 PROJECT OVERVIEW BINDER “A.3”

TABLE OF CONTENTS

- 1. INTRODUCTION**
 - a. Introduction Statement
 - b. Detailed Test Summary
- 2. COMPONENTS**
 - a. Components of the Diebold voting system package
- 3. RECOMMENDATION**
 - a. Recommendation Overview
 - b. Voting system application recommendation
 - c. Bar charts of residual failures
- 4. RESTRICTIONS**
 - a. Restrictions for use of the voting system
- 5. CONDITIONS**
 - a. Conditions for use of the voting system
- 6. COMMENTS**
 - a. Comments from testing board members
- 7. AUDIT REPORTS**
 - a. Testing Board response to audit report
 - b. Audit Report
 - c. Associated correspondence – Located in Binder “A”, Sec. 7
- 8. ADDITIONAL CORRESPONDENCE – Located in Binder “B”**

2007-CDOS-DIE-001-0402
PROJECT OVERVIEW BINDER “A.3”

INTRODUCTION

STATE OF COLORADO
Department of State

1700 Broadway, Suite 270
Denver, CO 80290



Mike Coffman
Secretary of State

Holly Lowder
Director, Elections

Why an Amendment to the A.2 binder/report?

Acting in accordance with HB08-1155, the Secretary of State requested the Testing Board to re-evaluate conditions after listening to testimony from county officials and the voting system vendor. Additionally, HB08-1155 allowed the Testing Board to consider county security procedures in the evaluation of the conditions for the voting system. The meetings, discussion and draft versions of the conditions were open to the public.

The sections of this binder have been modified to support the outcome of the additional testing.

Introduction - Original

On April 2, 2007, Diebold Election Systems (now known as Premier Election Solutions) approached the Colorado Secretary of State's Office with an application to certify a voting system. The application was accepted by the Voting Systems Certification Program Testing Board (Testing Board). The system was assigned certification number: 2007-CDOS-DIE-001-0402.

The voting system is known by its federal certification name as "GEMS 1-18-24." Federal certification is to the 2002VSS standards, and was obtained on June 27th, 2005 (NASED#: N-1-06-22-22-001).

The Testing Board proceeded to evaluate the Diebold voting system during the time period of April 2nd – December 1st. All findings are documented within the binders A – 30, as well as addendum binders 02.1 – 08.1, 13.1, 14.1, 16.1, 19.1, 20.1 – 23.1, 25.1, 25.2, 26.1 and 31.1.

The Project Overview Binders (Binders "A", "A.2", and "B") provides an overview of the findings of the project, and the following additional information:

- Introduction
- System Components
- Recommendation to the Secretary of State
- Restrictions on the use of the voting system suggested by the Testing Board
- Conditions to the Recommendation suggested by the Testing Board
- Additional Comments by the Testing Board
- Independent Audit Reports

During the process of certifying the system, the Testing Board adhered to the procedures outlined by the Voting System Program procedures document. The certification process was led by Michael Chadwell, with Geneice Mathews and Tim Bishop providing the primary cross evaluation. Additional cross check and documentation verification was conducted by Danny Casias with additional coordination by the Program Manager – John Gardner with assistance from Jerome Lovato as necessary.

The Testing Board evaluated the voting system in accordance with the requirements set forth in Secretary of State Rule 45, as well as applicable elements contained within the laws of the Help America Vote Act, Colorado Revised Statute, multiple sections of Title 1, and Secretary of State Rules as appropriate. All testing results and output which includes extensive video documentation of the evaluation process have been archived and well preserved in accordance with the Voting Systems Program procedures document.

Through the evaluation, the Testing Board identified a variety of deficiencies within the system which include functionality, security, auditability and documentation requirements. The following sections will address these deficiencies as either a restriction for use (preventing recommendation by the Testing Board), or a condition for use (allowing the system to be recommended provided conditional elements are adhered to). Restrictions are identified in a one-to-one value. One identified restriction = one failure on the Detailed Test Summary.

Conditional elements represent a one-to-many value. The execution of a single condition placed on the use of the system in many cases will address multiple failures as the Testing Board often experienced failures that exhibited a “daisy chain” effect. One high level failure would trigger many follow up test scenarios. Refer to the **Comments** section of this binder for additional comments on this topic.

STATE OF COLORADO
Department of State

1700 Broadway, Suite 270
Denver, CO 80290



Mike Coffman
Secretary of State

Holly Lowder
Director, Elections

Detailed Test Summary

The Testing Board executed the testing process for the Diebold voting system in the manner prescribed by Rule 45, and the detailed procedures document provided on the Voting Systems State Certification Program website (<http://www.elections.colorado.gov/DDefault.aspx?tid=501>).

The outcome of the process involved over 700 functional test evaluations, 4405 detailed line items for document review, and over 90 supplemental tests comprising the sections for application review, demonstration and work on completing the trusted build. The documentation comprised of this test work is evident in over 50 binders generated by the Testing Board, a multitude of boxes containing evidence generated from devices, ballots, reports, and other findings. In addition to this evidence, over 200 DVD records exist documenting the process of the Testing Board.

Below is the summary report of test status generated by the Testing Board regarding the Diebold Voting System evaluation:

Diebold						
	# Requirements	# Passed	# Failed	Binder Status	% Completed	% Passed
Phase I - Application	22	21	0	signed		95.45%
Phase II - Doc. Review	4405	3435	911	signed		77.98%
Phase III - Demo	54	54	0	signed		100.00%
Phase III - Trusted Build	20	20	0	signed		100.00%
Phase III - Functional Test (overall)	700	622	78		100.00%	88.86%
Security	139	115	24			82.73%
System Process	341	309	32			90.62%
Election (pre, ED and post)	220	198	22			90.00%
Independent Audit	1674	1674		Review of Test Board work.		100.00%
Phase IV - Certification Doc.	n/a	n/a	n/a	n/a	n/a	100.00%
Phase V - Qualification Report	n/a	n/a	n/a	n/a	n/a	100.00%

Requirements Status for Colorado Certification of Diebold Voting System

Section Category	Binder #	Category	Statute Code	Section C	Total # of Tests to complete	Status:	DRE	PCOS	CCOS	EMS	Remaining to complete
Section "A" - Pre Testing	1	Application	E	aa	22	Pass	n/a	n/a	n/a	18	0
						Pass Conditional	n/a	n/a	n/a	3	
						Suspend	n/a	n/a	n/a	1	
						Fail	n/a	n/a	n/a		
						Not applicable	n/a	n/a	n/a		
	2-6	Documentation Review	D	ab	4405	Pass	804	337	44	49	0
						Pass Conditional					
						Suspend					
						Fail	164	99	332	375	
						Not applicable	794	445	505	457	
	7	Demonstration	A	ac	54	Pass	14	13	13	14	0
						Pass Conditional					
						Suspend					
						Fail					
						Not applicable					
	8	Trusted Build	G	ad	20	Pass	4	4	4	2	0
						Pass Conditional		1	1		
						Suspend					
						Fail					
						Not applicable	1	1	1	1	
	9-12	Source Code Review		ae	0	Not applicable	n/a	n/a	n/a	n/a	0

Requirements Status for Colorado Certification of Diebold Voting System

Section Category	Binder #	Category	Statute Code	Section C	Total # of Tests to complete	Status:	DRE	PCOS	CCOS	EMS	Remaining to complete
Section "B" - Security Testing	13	System Access		ba	36	Pass	6	4	3	13	0
						Pass Conditional					
						Suspend					
						Fail		2	2	2	
						Not applicable	1	1	1	1	
	14	Operating System Security		bb	20	Pass				1	0
						Pass Conditional				1	
						Suspend					
						Fail					
						Not applicable	9			9	
	15	Database Security		bc	24	Not applicable	6	6	6	6	0
	16	Removable Media		bd	13	Pass	1	1		1	0
						Pass Conditional					
						Suspend					
						Fail				1	
						Not applicable	2	2	3	2	
	17	Networking and Telecommunications		be	46	Pass	6	2	5	5	0
						Pass Conditional					
						Suspend					
						Fail	4	8	1	4	
						Not applicable	2	2	5	2	

Requirements Status for Colorado Certification of Diebold Voting System

Section Category	Binder #	Category	Statute Code	Section C	Total # of Tests to complete	Status:	DRE	PCOS	CCOS	EMS	Remaining to complete
Section "C" - System Testing	18	System		ca	49	Pass	10	7		20	0
						Pass Conditional					
						Suspend					
						Fail		2		7	
						Not applicable				3	0
	18	System (central count)		cb	11	Pass	n/a	n/a	5	n/a	
						Pass Conditional	n/a	n/a		n/a	
						Suspend	n/a	n/a		n/a	
						Fail	n/a	n/a	1	n/a	
						Not applicable	n/a	n/a	5	n/a	0
	19-20	Ballot Process		cc	152	Pass	23	42	34	25	
						Pass Conditional	1				
						Suspend					
						Fail	1	2	4	1	
						Not applicable		2	8	9	0
	21	Performance		cd	24	Pass	2	2	1	4	
						Pass Conditional	6	3			
						Suspend					
						Fail			3	2	
						Not applicable			1		0
	21	DRE Processing *		ce	24	Pass	17	n/a	n/a	n/a	
						Pass Conditional		n/a	n/a	n/a	
						Suspend		n/a	n/a	n/a	
						Fail		n/a	n/a	n/a	
						Not applicable	7	n/a	n/a	n/a	0
	22	Audits		cf	29	Pass	6	5	4	6	
						Pass Conditional					
						Suspend					
						Fail		2		1	
						Not applicable	1	1	3		0
	22	Reports		cg	52	Pass	7	9	9	10	
						Pass Conditional					
						Suspend					
						Fail	3	2		1	
						Not applicable	3	3	3	2	0

Requirements Status for Colorado Certification of Diebold Voting System

Section Category	Binder #	Category	Statute Code	Section C	Total # of Tests to complete	Status:	DRE	PCOS	CCOS	EMS	Remaining to complete
Section "D" - Election Day Tests	23	Hardware Diagnostics Testing		da	8	Pass	2	1	1		0
						Pass Conditional					
						Suspend					
						Fail					
						Not applicable		1	1	2	0
	23	Voting		db	65	Pass	15	16	18	7	
						Pass Conditional					
						Suspend					
						Fail		1	2		0
						Not applicable	3	1	1	1	
	24	Multi-Page Ballots		dc	6	Pass		2	1	1	0
						Pass Conditional					
						Suspend					
						Fail					
						Not applicable	2				0
	24	Multiple Languages		dd	4	Pass	1	1	1	1	
						Pass Conditional					
						Suspend					
						Fail					0
						Not applicable					
	24	Provisional		de	25	Pass	2	3	3	3	0
						Pass Conditional			1		
						Suspend					
						Fail	4	1	1	2	
						Not applicable	1	2	1	1	0
	25	V-VPAT		df	28	Pass	26	n/a	n/a	n/a	
						Pass Conditional		n/a	n/a	n/a	
						Suspend		n/a	n/a	n/a	
						Fail	1	n/a	n/a	n/a	0
						Not applicable	1	n/a	n/a	n/a	
	25	Accessibility		dg	41	Pass	37	n/a	n/a	n/a	0
						Pass Conditional		n/a	n/a	n/a	
						Suspend		n/a	n/a	n/a	
						Fail	3	n/a	n/a	n/a	
						Not applicable	1	n/a	n/a	n/a	0
	26	Closing Polls		dh	30	Pass	12	12	n/a	n/a	
						Pass Conditional			n/a	n/a	
						Suspend			n/a	n/a	
						Fail	3	3	n/a	n/a	0
						Not applicable			n/a	n/a	

Requirements Status for Colorado Certification of Diebold Voting System

Section Category	Binder #	Category	Statute Code	Section C	Total # of Tests to complete	Status:	DRE	PCOS	CCOS	EMS	Remaining to complete
Section "E" - Post Election	27	Post Election Audit *		ea	4	Pass	1	1	1	1	0
						Pass Conditional					
						Suspend					
						Fail					
						Not applicable					0
	27	Recount		eb	8	Pass	2	1	3	1	
						Pass Conditional	1				
						Suspend					
						Fail					0
						Not applicable					
	27	Recount (central count)		ec	1	Pass	n/a	n/a		n/a	0
						Pass Conditional	n/a	n/a		n/a	
						Suspend	n/a	n/a		n/a	
						Fail	n/a	n/a	1	n/a	
						Not applicable	n/a	n/a		n/a	0
Documentat	28	Video Documentation Log									
	29	Safe Documentation Log									
	30	Other Notes/Logs									

Archive Storage Boxes for the Diebold Voting System Certification Process:



Backup Binders documenting the Diebold Voting System Certification Process – (original binders moved to archive storage upon completion of process):



2007-CDOS-DIE-001-0402
PROJECT OVERVIEW BINDER “A.3”

COMPONENTS

STATE OF COLORADO
Department of State

1700 Broadway, Suite 270
Denver, CO 80290



Mike Coffman
Secretary of State

Holly Lowder
Director, Elections

Components

As submitted on April 3, 2007, the following components comprise the requested voting system package from Premier Election Systems (formerly Diebold Election Systems):

Component Name	System Function	Version Number
GEMS	Software Application	1.18.24
Accuvote OS Model "D"	Precinct Optical Scanner	1.96.6
Accuvote OS Model "D"	Central Count Optical Scanner	2.0.12
Accuvote TSx Model "C" & "D" w/ V-VPAT	Direct Record Electronic Device	4.6.4
VC Programmer	Voter Card Activation Interface for DRE.	4.6.1
Voter Card Encoder	Hand held Voter Card Activation unit for DRE.	1.3.2
Key Card Tool	Software application used for managing secure keys between DRE voting Devices	4.6.1

Photographs and additional details on each component can be found under test # AA6-P1-605.

2007-CDOS-DIE-001-0402
PROJECT OVERVIEW BINDER “A.3”

RECOMMENDATION

STATE OF COLORADO
Department of State

1700 Broadway, Suite 270
Denver, CO 80290



Mike Coffman
Secretary of State

Holly Lowder
Director, Elections

Recommendation Overview

The approach of the Testing Board regarding a recommendation is absolute. Any one item outstanding in the Restrictions section of the binder (no “conditional use” option discoverable by the Testing Board) will trigger a “N” value on the **Recommendation** table.

Therefore, for quick understanding of the overall outstanding deficiencies with the system, and to provide a summary of reasons for the “Y” or “N” value in the **Recommendation** table.

The following table provides a high level summary statement of findings by the Testing Board. These items constitute a summary of the findings in the **Restrictions** section of the project overview binder.

Component (details in the components section)	Recommended to be Certified?	Reason
Software (1-18-24)	No	<ul style="list-style-type: none">• Failure to prove Federal Testing was conducted• Failure to provide required State Documentation
Precinct Scanner (1.96.6)	No	<ul style="list-style-type: none">• Failure to provide required State Documentation• Machine mis-feeds were tested outside of acceptable levels
Central Count Scanner (2.0.12)	No	<ul style="list-style-type: none">• Failure to prove Federal Testing was conducted• Failure to provide required State Documentation• Machine mis-feeds were tested outside of acceptable levels
DRE (4.6.4 C&D)	No	<ul style="list-style-type: none">• Failure to provide required State Documentation• Paper Record not accessible to blind voters.



Diebold Election Systems Recommendation for Voting System Application:

2007-CDOS-DIE-001-0402

Updated 4/4/08

Binary Assessment plus N/A (Y/N, with conditionals)

<u>Component</u>	<u>Version</u>	<u>Accuracy</u>	<u>Security</u>	<u>Accessibility</u>	<u>Compliance</u>	<u>Test Board Recommendation</u>
GEMS	1.18.24	Y ³	Y ³	N/A	N ^{1, 2}	N
AVOS CC	2.0.12	Y ³	Y ³	N	N ^{1, 2}	N
TSX-C	4.6.4	N ³	Y ³	N	N ²	N
TSX-D	4.6.4	N ³	Y ³	N	N ²	N
AVOS PC	1.96.6	N ³	Y ³	N	N ²	N

¹ Colorado Revised Statutes Title 1, Article 5, Section 6 (1-5-608.5) prohibits allowing certification of voting equipment by the Secretary of State if it has not been successfully qualified by a recognized ITA. Additionally, Rule 45.5.1.3 requires voting systems to be compliant with federal requirements.

² Missing/Insufficient state documentation pursuant to Colorado Secretary of State Rule 45.

³ Provided jurisdictions follow additional procedural steps outlined in the **Conditions** section to mitigate the deficiencies of the system as evaluated. Should conditions not be applied or adhered to as indicated in this binder, the Testing Board would reject the system and modify the value to a "N." This is specifically addressed in the Testing Board comments section of this binder.

Definitions:

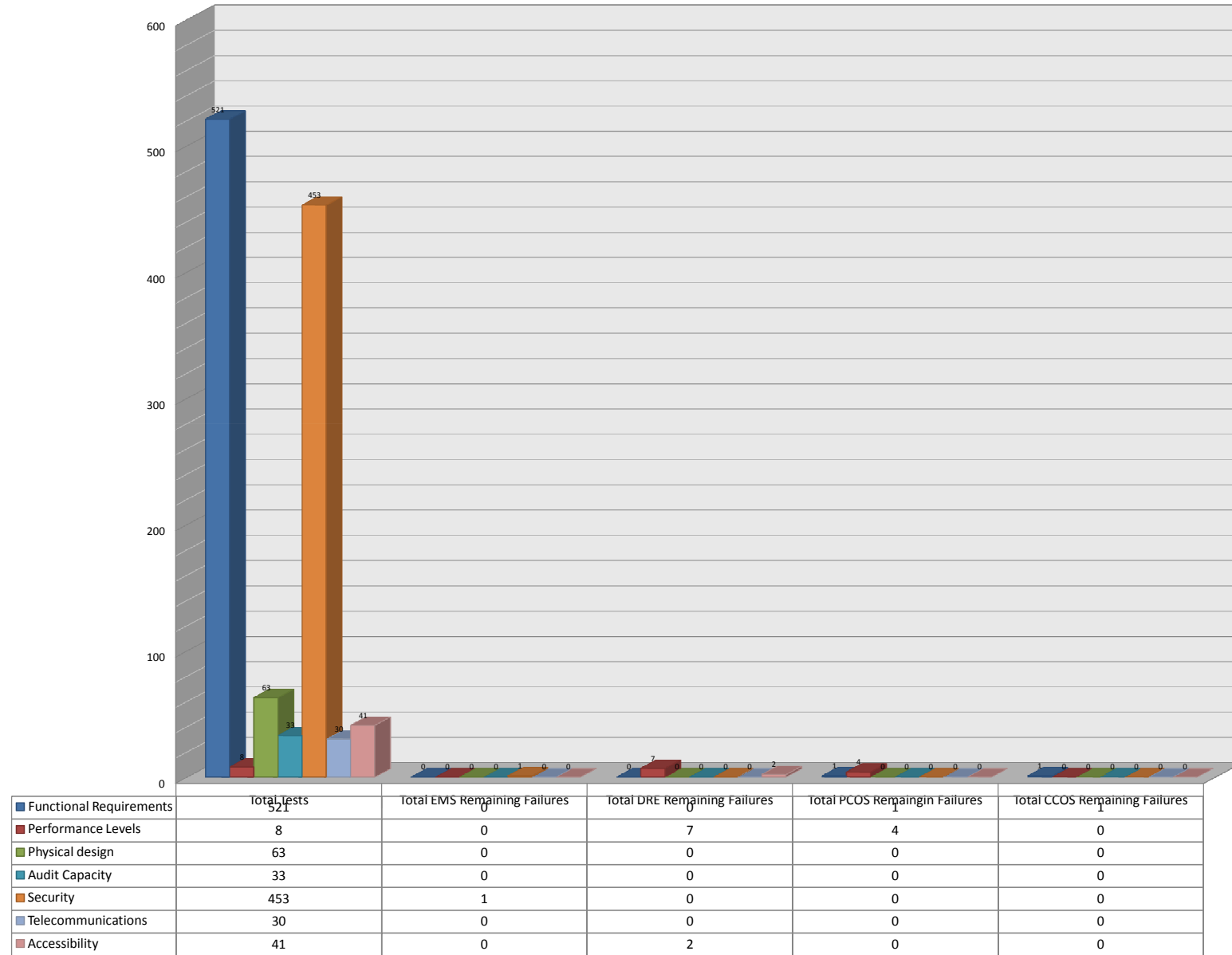
Accuracy – correctly reading, displaying, tabulating and reporting votes. (Functional, or Performance)

Security – vote data is protected and maintains integrity throughout system processing. (Audit, Security, or Telecommunications)

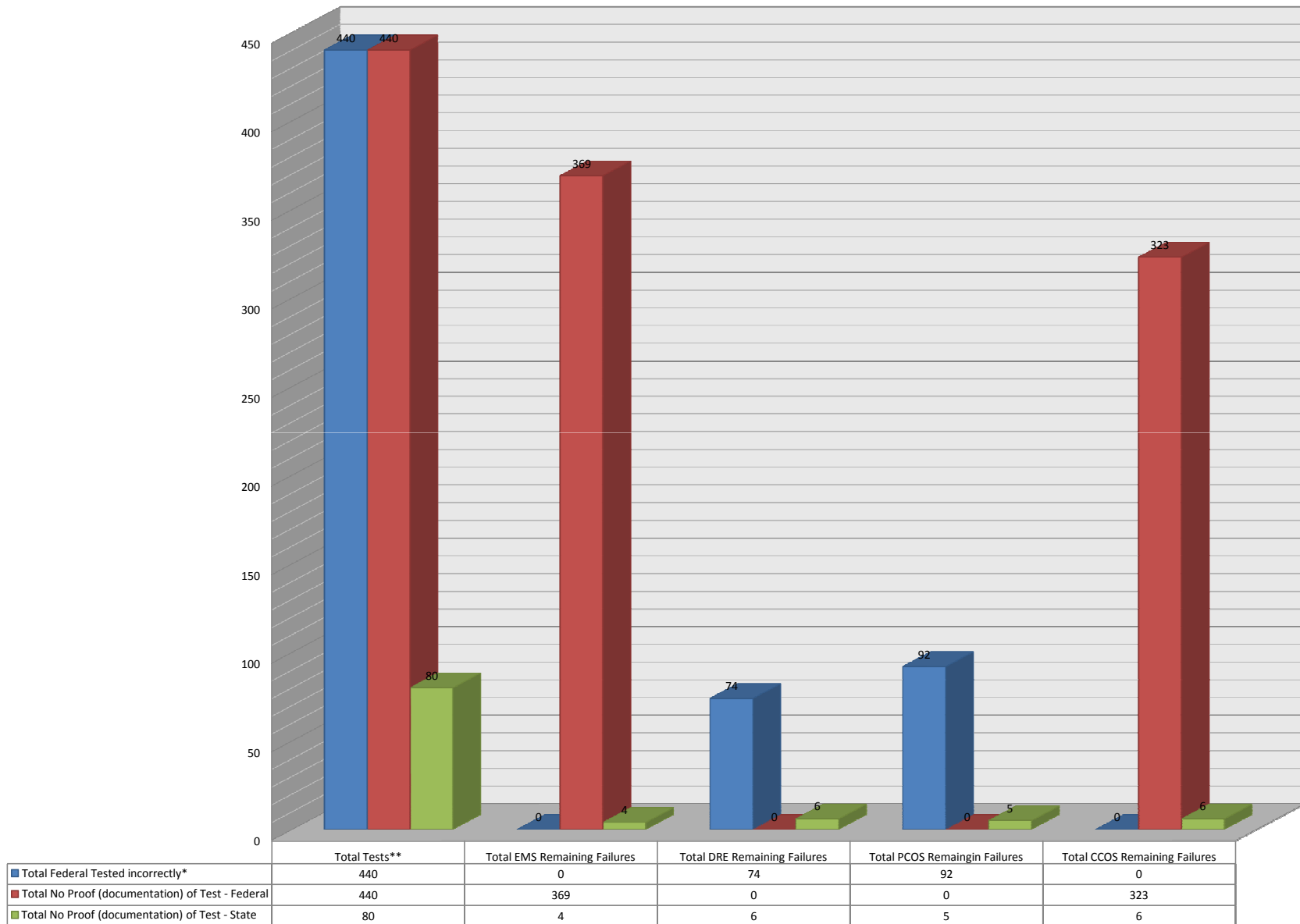
Accessibility – voter systems have requisite usability and reliability. (Functional, Accessibility, or Physical Design)

Compliance – systems conform to federal and state requirements for certification and/or documentation. (Documentation)

Diebold Failure Status by Category



Diebold Documentation Failure Status by Category



* Incorrectly tested means the ITA either reported that a required item was not tested, or a required item was tested incorrectly for the device type.

** Total tests has N/A items removed for chart scale.

2007-CDOS-DIE-001-0402
PROJECT OVERVIEW BINDER “A.3”

RESTRICTIONS

STATE OF COLORADO
Department of State

1700 Broadway, Suite 270
Denver, CO 80290



Mike Coffman
Secretary of State

Holly Lowder
Director, Elections

The Testing Board has identified the following items as deficient in the voting system, requiring restriction for use of the voting system components based on the review and testing of the voting system for compliance with state requirements:

Software Restrictions:

GEMS 1.18.24 –

1) Documentation

Insufficient federal/state certification compliance testing and/or documentation, i.e. 2002 VSS requirements matrix.

Rule

Text

CRS 1-5-601.5

Compliance with federal requirements. All voting systems and voting equipment offered for sale on or after May 28, 2004, shall meet the voting systems standards that were promulgated in 2002 by the federal election commission and that may thereafter be promulgated by the federal election assistance commission. Subject to section 1-5-608.2, nothing in this section shall be construed to require any political subdivision to replace a voting system that is in use prior to May 28, 2004.

45.5.1.1

All voting systems shall meet the voting systems standards pursuant to section 1-5-601.5, C.R.S., and Secretary of State Rule 37.3.

45.5.2.4.2

All VSTL qualification reports, test logs, and technical data packages shall be evaluated to determine if the voting system meets the requirements of this rule and have completed the applicable federal certification requirements at the time of State testing. Failure to provide such documentation of independent testing will result in the voting system application being rejected

45.5.2.3.19

(d) The voting system provider shall deliver to the Secretary of State documentation detailing estimated time of operation on battery for each type of optical scanner, ballot imager, DRE, and V-VPAT they provide, assuming continuous use of the devices by voters during an interruption of normal electrical power.

45.5.2.4.1

In addition to other documentation requirements in this rule, the voting system provider shall provide the following documents:

(c) Training Manual (and materials);

45.5.2.7.10

Voting systems providers shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the voting system provider will use to:

(c) Develop responsive updates to the system and/or corrective procedures;

Precinct Count Scanner Restrictions:

AVOS PC Version 1.96.6 –	Rule	Text
1) Functional Requirements Ballot handling errors: misfeeds (<= 1 per 5000) and corrective action reporting. Device tested outside of acceptable criteria.	45.6.2.3.15	The system shall stop and inform operator of ballot handling errors such as misfeeds, damaged ballot, and multiple feeds. Also, give corrective measures to remove the ballot, sort is as unreadable (out stack) and gives a way to restart or recount the uncounted ballots. (Misfeeds =< 1 per 5,000).
2) Documentation	45.5.1.2	All voting system software, hardware, and firmware shall meet all requirements of federal law that address accessibility for the voter interface of the voting system. These laws include, but are not necessarily limited to, (a) the Help America Vote Act.
	45.5.2.3.2	The voting system shall meet the following environmental controls allowing for storage and operation in the following physical ranges: (a) Operating – Max. 95 Degrees Fahrenheit; Min 50 Degrees Fahrenheit, with max. humidity of 90%, normal or minimum operating humidity of 15%. (b) Non-Operating – Max. 140 Degrees Fahrenheit; Min. 4 Degrees Fahrenheit. Non-operating humidity ranges from 5% to 90% for various intervals throughout the day. The material supplied by the voting system provider shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, telecommunications service, and any other facility or resource required for the installation, operation, and storage of the voting system.
	45.5.2.4.1	In addition to other documentation requirements in this rule, the voting system provider shall provide the following documents: (c) Training Manual (and materials);
	45.5.2.7.10	Voting systems providers shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the voting system provider will use to: (c) Develop responsive updates to the system and/or corrective procedures;

AVOS PC Version 1.96.6 –

3) Performance

Rule

45.5.2.3.19

Text

All electronic voting devices provided by the voting system provider shall have the capability to continue operations and provide continuous device availability during a period of electrical outage without any loss of election data.

(a) For optical scan devices, this capability shall include at a minimum for a period of not less than three (3) hours the ability to:

- (i) Continue to scan or image voters' ballots;
- (ii) Tabulate accurately voters' choices from the ballots;
- (iii) Store accurately voters' ballot choices during a period of electrical outage; and
- (iv) Transmit required results files accurately if power failure experienced during transmittal of results.

DRE Restrictions:

TSX(C, D) w/V-VPAT 4.6.4 –

1) Documentation

Rule

Text

45.5.1.2

All voting system software, hardware, and firmware shall meet all requirements of federal law that address accessibility for the voter interface of the voting system. These laws include, but are not necessarily limited to,

(a) the Help America Vote Act, and

(c) the Federal Rehabilitation Act. The voting system provider shall acknowledge explicitly that their proposed software, hardware, and firmware are all in compliance with the relevant accessibility portions of these laws.

45.5.2.3.2

The voting system shall meet the following environmental controls allowing for storage and operation in the following physical ranges:

(b) Non-Operating – Max. 140 Degrees Fahrenheit; Min. 4 Degrees Fahrenheit. Non-operating humidity ranges from 5% to 90% for various intervals throughout the day.

45.5.2.4.1

In addition to other documentation requirements in this rule, the voting system provider shall provide the following documents:

(c) Training Manual (and materials);

45.5.2.7.10

Voting systems providers shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the voting system provider will use to:

(c) Develop responsive updates to the system and/or corrective procedures;

45.5.2.8.2

Documentation of the accessibility of the voting system shall include the following items at a minimum:

(c) Technology used by the voting system that prevents headset/headphone interference with hearing aids;

2) Accessibility

37.1.4

The voting systems described in the foregoing paragraphs shall produce a record with an audit capacity for such system.

(d) The paper record shall be accessible for individuals with disabilities including non-visual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters.

45.5.2.9.10

The V-VPAT device shall be designed to allow every voter to review, and accept or reject his/her paper record in as private and independent manner as possible for both disabled and nondisabled voters.

TSX(C, D) w/V-VPAT 4.6.4 –**3) Performance****Rule**

45.5.2.3.19

Text

All electronic voting devices provided by the voting system provider shall have the capability to continue operations and provide continuous device availability during a period of electrical outage without any loss of election data.

(b) For DRE devices, this capability shall include at a minimum for a period of not less than three (3) hours the ability to:

(i) Continue to present ballots accurately to voters;

(ii) Accept voters' choices accurately on the devices;

(iii) Tabulate voters' choices accurately;

(iv) Store voters' choices accurately in all storage locations on the device; and

(v) Transmit required results files accurately if power failure is experienced during transmittal of results.

(c) For V-VPAT devices connected to DREs, this capability shall include at a minimum for a period of not less than three (3) hours the ability to:

(i) Continue to print voters' choices on the DRE accurately and in a manner that is identical to the manner of the printers' operations during a period of normal electrical operations; and

(ii) Continue to store the printed ballots in a secure manner that is identical to the manner of the printers' operations during a period of normal electrical operations.

Central Count Scanner Restrictions:

AVOS CC 2.0.12 –	Rule	Text
1) Functional Requirements Ballot handling errors: misfeeds (<= 1 per 5000) and corrective action reporting. Device tested outside of acceptable criteria.	45.6.2.3.15	The system shall stop and inform operator of ballot handling errors such as misfeeds, damaged ballot, and multiple feeds. Also, give corrective measures to remove the ballot, sort is as unreadable (out stack) and gives a way to restart or recount the uncounted ballots. (Misfeeds =< 1 per 5,000).
2) Documentation Insufficient federal/state certification compliance testing and/or documentation.	CRS 1-5-601.5	Compliance with federal requirements. All voting systems and voting equipment offered for sale on or after May 28, 2004, shall meet the voting systems standards that were promulgated in 2002 by the federal election commission and that may thereafter be promulgated by the federal election assistance commission. Subject to section 1-5-608.2, nothing in this section shall be construed to require any political subdivision to replace a voting system that is in use prior to May 28, 2004.
	45.5.1	All voting systems shall meet the voting systems standards pursuant to section 1-5-601.5, C.R.S., and Secretary of State Rule 37.3.
	45.5.2.4.2	All VSTL qualification reports, test logs, and technical data packages shall be evaluated to determine if the voting system meets the requirements of this rule and have completed the applicable federal certification requirements at the time of State testing. Failure to provide such documentation of independent testing will result in the voting system application being rejected.
	45.5.1.2	All voting system software, hardware, and firmware shall meet all requirements of federal law that address accessibility for the voter interface of the voting system. These laws include, but are not necessarily limited to, (a) the Help America Vote Act
	45.5.2.3.2	The voting system shall meet the following environmental controls allowing for storage and operation in the following physical ranges: (a) Operating – Max. 95 Degrees Fahrenheit; Min 50 Degrees Fahrenheit, with max. humidity of 90%, normal or minimum operating humidity of 15%. (b) Non-Operating – Max. 140 Degrees Fahrenheit; Min. 4 Degrees Fahrenheit. Non-operating humidity ranges from 5% to 90% for various intervals throughout the day. The material supplied by the voting system provider shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, telecommunications service, and any other facility or resource required for the installation, operation, and storage of the voting system.
	45.5.2.4.1	In addition to other documentation requirements in this rule, the voting system provider shall provide the following documents: (c) Training Manual (and materials);

AVOS CC 2.0.12 –

(Documentation continued.)

Documentation was not provided by the voting system vendor to allow testing board to evaluate this requirement.

Rule

45.5.2.7.10

Text

Voting systems providers shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the voting system provider will use to:

(c) Develop responsive updates to the system and/or corrective procedures;

VC Programmer Restrictions:

Version 4.6.1 – NO RESTRICTIONS

Voter Card Encoder Restrictions:

Version 1.3.2 – NO RESTRICTIONS

Key Card Tool Restrictions:

Version 4.6.1 – NO RESTRICTIONS

2007-CDOS-DIE-001-0402
PROJECT OVERVIEW BINDER “A.3”

CONDITIONS

STATE OF COLORADO
Department of State

1700 Broadway, Suite 270
Denver, CO 80290



Mike Coffman
Secretary of State

Holly Lowder
Director, Elections

FINAL – 4/4/2008

Conditions for Use – PREMIER - AMENDED 4/4/08

The Testing Board recommends that the Secretary of State adopt the following conditions for use of the voting system. These conditions are required to be in place should the Secretary approve for certification any or all of the items indicated in the **COMPONENTS** section. The Testing Board has modified the conditions based on information provided through public hearing under legislative updates to consider additional procedures. Any deviation from the conditions provides significant weakness in the security, auditability, integrity and availability of the voting system.

Global Conditions (applies to all components):

- 1) Modem and other telecommunication devices may not be used on any subsystem component - system provider was unable to meet or provide prerequisite FIPS 140/180 certifications.
- 2) Provisional ballots must be processed separately from non-conditional ballots - system subcomponents are unable to functionally differentiate and correctly process to Colorado specific requirements.
- 3) Coordination of Escrow Setup - Upon Certification, voting system manufacturer must coordinate the Escrow of the TRUSTED BUILD software with SOS escrow, or third party escrow service as required by Rule 11 prior to use in Colorado.
- 4) Abstract Report generation - abstracts used for State reporting must come from GEMS Software, or other external solution, rather than from the specific device.
- 5) Trusted Build Verification
Counties shall ensure that hardware, software and firmware purchased for use of the system matches the specifications of VSTL/EAC and/or State Certified and trusted versions, not to the version presented in the vendor documentation.
- 6) Counties using the voting system shall testify through their security plan submission that the voting system is used only on a closed network.

Software Conditions (GEMS 1-18-24):

- 1) System/Database/Network Security Hardening.
 - a) Because the voting system operates in a non-restricted system configuration containing open file system access to locate, copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions. Counties shall submit their plan for approval to the Secretary of State's office to be included in the County Security Plan on overcoming these conditions through county environmental and/or procedural changes where possible.
 - b) In addition to physical environmental changes, counties shall create a second (or backup) copy of the GEMS database that is created immediately after the point of memory card downloads. The backup copy shall be stored on closed CD Media and documented as matching the master database. This process shall be observed by two election staff members. Chain of custody documents shall be generated for the media, and the media shall be sealed with at least two tamper evident seals and stored in a sealed or lockable transfer case that is stored in a limited access area. On election day, the designated election official shall load the sealed copy of the database onto the server and proceed with uploading memory cards after documenting the loading of the backup master database onto the system. After loading the sealed database copy, the county shall re-secure the database with seals (updating necessary logs) in the limited access location.
 - c) Additionally, to overcome deficiencies in security and auditing of the system, the county will be required to perform increased Election Night and Post Election Audits for this system. All post-election audit data shall process a hand count of paper ballots which shall match the totals report from the specific device, as well as the totals for the GEMS database. Counties shall prepare for this event with one of two methods:

Option #1 – Prepare for the upload of memory cartridges as normal. Print necessary zero report. Upon uploading each individual memory card, print a summary report showing the change in totals from the upload of the memory card. Label the report to match the name/number of the memory card uploaded. Continue to upload memory cards and print totals reports to match. When auditing a specific device, use the difference between the report totals for the memory card selected for the audit and the totals from the immediately preceding memory card report to calculate vote totals generated by the GEMS software.

When memory cards are delivered to the county for upload, the machine generated report shall be delivered for inspection as well. During the post-election audit the summary report indicated above is created, the difference totals (delta report) are compared to the totals from the report generated by the device at the polling place. If the reports match, the public and canvass board is ensured that the totals from the polling place match the totals from the county server. If the totals are different, the county is to report the situation to the Secretary of State's office for audit, security and remedy procedures.

During the post election audit process, the totals of the paper record for the specific device are to be hand counted and verified against the electronic record for the device. The canvass board shall report the verification of three totals to match – the paper record of the device, the totals of the electronic vote on the device, and the totals in the central count server; OR

Option #2 – Prepare for the upload of memory cartridges by creating one master default database (containing all memory cards/cartridges). Create individual databases to contain values (upload data) for each separate memory card (or in some instances by batch of ballots – see condition #4b under Central Count devices. Upload memory card/cartridges into master database, and into the specific database created for that memory card (two separate uploads). This process can take place any time after the close of polls including through the canvass period, with observation by at least two people. Election summary reports shall be printed from each individual database and manually added together. The totals from the individual databases must match the master database before proceeding. Upon verification that the master and individual databases match, the county can then use the individual reports to conduct a hand count of the paper ballot (or paper record) generated by the device to show that the GEMS totals match. The verification of the separate upload databases verify that the database totals match the field totals on each memory card device, as was designed after the point of Logic and Accuracy testing took place.

2) Ballot-On-Demand Restriction.

No provision for ballot reconciliation. This will require counties to have an extra supply of preprinted ballots on hand. Alternatively the county may use the system for ballot on demand printing provided that detailed logs are maintained indicating the number of ballots printed, used and not used by the in-house printing function.

3) Audit Trail Information:

a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the GEMS software for processing by other methods.

b) Operators of the system shall also be required to maintain logs indicating use of the report printing functions of the software, and detailed information to changes of the system including hardware changes which shall include: insert removable media, remove removable media, modify system hardware drivers, modify system physical hardware, and any other system property changes made by either judges or other trusted staff. Logs shall be maintained physically in a file outside or separate from the database, which is NOT accessible for review and/or modification by user/operator accounts on the system, but that is readily accessible to election officials or other interested party.

Such logs may be achievable by a manner best suitable to each county. Solutions may include the use of key stroke recording software, windows event log recordings, detailed video camera recordings, manually written records, or any combination to achieve the necessary audit data. Counties shall report to the Secretary of State's office through their security plans the method of achieving this condition.

4) Performance Deficiencies.

Due to failures in performance, counties shall allow extra time for downloads and uploads of memory card devices. This may impact programming, testing, and use of the system on election night. Counties shall ensure trusted staff is properly trained on this issue and accommodating the allowable time required for programming memory devices.

5) Provisional Ballots.

The software is not capable of processing provisional ballots internally to accept federal and state only questions. A procedure outside of the voting system will be required. Additionally, the abstracts and

reports created by the software do not meet the requirements of rule 41.6.3(g) and users of the system will be required to generate an abstract outside of the voting system.

Precinct Count Scanner Conditions (1.96.6):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Due to limitations by device to verify Trusted Build once installed, counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State.

2) Device Security Accessibility.

a) Device level administrative functions requiring access involving the use of keys, memory cards, Ender cards (closing polls) and passwords must be restricted to no more than two (2) person entry with detailed logs.

b) Due to exposure of passwords, the vendor and the county shall ensure that operators are adequately trained to protect the visibility of the password during use.

3) Ballot/Race Conditions Simulation.

Additional County testing shall be required to accommodate ballots with conditions from each election. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

4) Audit Trail Information:

a) Judges shall be required to include device serial number on all reports regarding use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

b) Operators of the system shall also be required to maintain logs indicating use of the administrator functions of the device by either judges or other trusted staff.

c) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the GEMS software for processing by other methods.

d) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper ballots to match the totals generated from the GEMS software as indicated in Software condition #1c.

Central Count Scanner Conditions (2.0.12):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Due to limitations by device to verify Trusted Build once installed, counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State.

2) Ballot Processing.

- a) Counties will be required to pre-process all folded ballots that are counted by the voting device. Specifically, operators will presort ballots to detect for appearances of holes punched in the ballot. Ballots with holes in them shall be duplicated onto new ballots by a duplication board as required. Operators of the system shall be adequately trained in the processing and understanding of error messages produced by the device which sometimes represent the correct problem and many times do not.
- b) In the event of a recount, the county will have the voting system technician on-site to recalibrate the scanning devices to the sensitivity settings required for testing the device as required by Secretary of State Rule 27.4.2(d). Alternatively, the counties shall perform necessary testing to document and demonstrate that the auto-calibration feature of the device is functioning prior to the counting of ballots for the recount.

3) External Power Supply Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendors' recommendation for the component. Acceptable power supply sources include generators and other facility based solutions.³

4) Audit Trail Information:

- a) Judges shall be required to include device serial number on all reports regarding use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.
- b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include a hand count of at least the following amounts of ballots counted on the device for the specific races selected in the post election audit:

Total # of Ballots Counted on Device:	Total # of Ballots to audit:	# of errors requiring escalation:
150,000 to 500,000	1,250	6
35,001 to 150,000	800	4
10,001 to 35,000	500	3
3,201 to 10,000	315	2
1,201 to 3,200	200	2
501 to 1,200	125	2
281 to 500	80	1
151 to 280	50	1
91 to 150	32	1
51 to 90	20	1
26 to 50	13	1
16 to 25	8	1
9 to 15	5	1
1 to 8	3 or 100% if less than 3	1

Errors detected during the manual audit process shall be resolved according to C.R.S. 1-7-514, and Secretary of State Rule 11. Errors discovered exceeding the error rate identified in the table above shall require escalation measures including increased audits as prescribed by the Secretary of State's office. County officials shall contact the Secretary of State's office as soon as possible if an audit detects errors above the escalation threshold.

The verification of the hand count of paper ballots shall match the totals generated from the GEMS software as indicated in Software condition #1c. Counties shall load only the master database from the secured storage location for processing the post election audit ballots as indicated in Software Condition #1b. Counties shall prepare database and batches of ballots prior to scanning into system (for election results) to accurately generate reports in batch sizes as necessary for the audit.

5) Ballot/Race Conditions Simulation.

Additional County testing shall be required to accommodate ballots with conditions listed. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

6) Network Access/Availability.

The voting system must be used with no network connectivity between devices/units and software. Only a closed LAN connection may be used with necessary hardware for port replication and local IP address assignments as tested.

DRE Conditions (TSx 4.6.4 – C and D models):

1) V-VPAT Paper Record Shall be Handled per Rule 11.6.

- a) Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation. Counties shall follow the requirements for handling according to Secretary of State Rule 11 and 43.
- b) Election judges are required to perform the “Printer Test” in between paper changes and verify with one additional judge that the paper has been loaded correctly and is printing according to design which ensures that all machines will have paper records for each vote cast.

2) Accessible Distances.

Operators of the system shall be required to provide an accessible solution by operating the device on a separate table. The manufacturer’s stand does not meet accessible reaches as outlined in C.R.S. 1-5-704. Counties shall be educated on these measurements and ensuring that the table top solution complies with the requirements. This condition could also be achieved with the use of a reach stick that is at least 4” in length. Should the counties use the DRE in the stand with a reach stick, the county shall ensure that a side approach by a wheelchair is possible due to the deficiencies in the knee clearance (depth and width) of the stand.

3) Accessible Operation.

Due to the inability for the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voters and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

4) Additional Privacy Screen Required.

Required privacy conditions can not be met with attached device privacy panels without also installing accessory screen made by manufacturer; alternatively this condition could be achieved with the use of a computer monitor polarized privacy screen. Counties shall deploy touch screen units in such a manner that voters and judges cannot easily walk behind other voters while processing their vote.

VC Programmer Conditions:

Version 4.6.1 – NONE

Voter Card Encoder Conditions:

Version 1.3.2 – NONE

Key Card Tool Conditions:

Version 4.6.1 – NONE

2007-CDOS-DIE-001-0402
PROJECT OVERVIEW BINDER “A.3”

COMMENTS



Testing Board Comments

The test board has unveiled a known reality that no computer system is perfect. Additionally, we have discovered and documented that no system can currently meet the requirements of Rule 45 as applied in its' strictest sense. Where possible, the Testing Board attempted to overcome these deficiencies in the form of "conditions for use" of the system – procedural workarounds.

The Testing Board recognizes that the conditions created are in essence a "last resort" workaround to accommodate requirements that do not meet specific sections of Colorado Revised Statutes 1-5-615. The preference of the Testing Board would be to have the specific deficiencies addressed with a system solution as required. Given the ability to mitigate deficiencies with procedural workarounds (C.R.S. 1-5-621), the Testing Board presents conditional use scenarios in the "**Conditions**" section that are directly tied to the recommendation status. Being that many workarounds address the security, auditability and availability of the system component, the Testing Board would firmly reject any option which removes, replaces or diminishes the conditional requirement and still allow the system to be used and recommended for certification. Any "Y" value in the **Recommendation** table would change to a "N" value with any change to the conditions.

These conditional procedures rely heavily on proper execution by county administrators and/or election judges. While we have faith that these dedicated workers will attempt to perform their duties to the best of their abilities, a majority of the conditions involve a human element which may or may not produce the acceptable outcome. This single factor alone causes concern that a security issue may not be resolvable in a post-election scenario.

Finally, it is of value to point out that the conditions that address security specific events are only addressing the attack scenario of a change in vote totals (refer to Cyber Security Report). The essence of the workaround in this case is to ensure that the vote totals calculated electronically are a match to the paper records. This requires absolute assurance that all paper records exist and are auditable for a successful outcome and high confidence in the report of votes by any given county.